REMARKS/ARGUMENTS

Favorable reconsideration of this application is respectfully requested.

Claims 1, 2, and 4-19 are pending in this application. Claims 1, 2, 4-11, and 17-19 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. patent 5,640,456 to Adams, Jr. et al. (herein "Adams") in view of "A Solution to Wireless Connections in a Multi-Bus Network" to Sato et al. (herein "Sato") and further in view of "5C Digital Transmission Content Protection White Paper" to Hitachi et al. (herein "Hitachi"). Claims 12 and 13 were rejected under 35 U.S.C. § 103(a) as unpatentable over Adams in view of U.S. patent 5,175,765 to Perlman and further in view of Hitachi. Claims 14-16 were rejected under 35 U.S.C. § 103(a) as unpatentable over Adams in view of Hitachi.

Addressing the above-noted prior art rejections, those rejections are traversed by the present response.

Initially, applicants note the claims are amended by the present response to clarify features recited therein. Specifically, independent claim 1 now clarifies the "contents protection information transfer unit" operates "to selectively relay the contents protection information transparently" without making any changes in the contents protection information. Independent claim 2 is similarly amended.

Further, independent claim 5 is amended by the present response to clarify that the "second contents protection unit" carries out the contents protection procedure "separately from the contents protection procedure carried out by the first contents protection unit". Independent claims 11, 17 and 19 are similarly amended as in independent claim 5.

The claims as currently written are believed to distinguish over the applied art.

Each of the above-noted rejections cites Adams as a primary reference. However, applicants respectfully submit the claims differ in significant ways from the teachings in Adams, Adams could not be properly modified to meet the claim limitations, and further no

combination of teachings of Adams in view of Sato and Hitachi, or in view of Perlman and Hitachi, or in view of Hitachi, would fully meet the claim limitations.

Adams discloses an encryption/decryption device, which is to be spliced in a single local area network. Adams is not directed to an encryption/decryption device between two networks operated under different protocols, and further the mere showing of two networks operated under different protocols as in Sato does not provide any motivation to combine such a feature in Sato into the teachings of Adams because such a combination makes no sense in the context of the device of Adams. Similarly, Adams completely fails to disclose or suggest any features related to a contents protection procedure in any way, and thereby a mere showing of a contents protection procedure including an authentication and/or a key exchange in Hitachi does not set forth any motivation to combine such a feature of Hitachi with the teachings of Adams as such teachings in Hitachi have no relevance to the device of Adams. Further, as discussed in more detail below, Adams fails to teach or suggest several features positively recited in the claims.

The applicants of the present invention set forth providing a relay device between two networks operated by different networks, for example to handle copyright protection information effectively under such a network environment. The cited art does not even address such features.

More specifically, Adams discloses an encryption/decryption device, which is to be spliced in a local area network, and which selectively encrypts or decrypts only a data portion of a data packet, leaving routing information contained in header and trailer portions of the data packet unchanged (see the Abstract in Adams).

The claims are not at all directed to such an encryption/decryption device that selectively encrypts/decrypts only a data portion, without encrypting/decrypting routing information in a header.

In contrast to a device such as in Adams, the claims are directed to a relay device that handles contents protection information that is necessary in carrying out a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on a first network and another device/service/sub-unit on a second network, or a relay device that carries out a contents protection procedure including at least an authentication and/or a key exchange, separately with respect to one device/service/sub-unit on the first network and with respect to another device/service/sub-unit on the second network.

In this respect, Adams completely fails to disclose or suggest any contents protection procedure including at least an authentication and/or a key exchange. The basis for the outstanding rejection appears to be confusing a contents protection procedure with encryption/decryption. In that respect, applicants note authentication and/or key exchange are known procedures to be carried out between two nodes that wish to communicate with each other, for authenticating each other or sharing a key to be used for encryption/decryption. These procedures themselves do not encrypt/decrypt anything, and are thereby distinct from an actual encryption/decryption.

Adams is directed to encryption/decryption and not to authentication and/or key exchange. The outstanding rejection cites several portions in Adams directed to encryption/decryption as meeting limitations for the authentication and/or key exchange between a device/service/sub-unit on a first network and another device/service/sub-unit on a second network, and particularly the Office Action cites teachings in Adams at column 4, lines 40-52; column 5, lines 2-5; column 5, line 61 to column 6, line 5; column 6, lines 6-16 and 21-29; and column 6, line 65 to column 7, line 11.[1]

[1] See for example the discussion in the Office Action of February 11, 2005, at pages 2-4 with respect to the rejection of Claim 1.

However, applicants respectfully submit the teachings in Adams do not correspond to the claimed features.

At column 4, lines 40-42, Adams merely discloses a table being used in making a routing or encryption/decryption decision, which includes keys for encrypting and decrypting data. That disclosure in Adams does not even mention any authentication or key exchange.

At column 5, lines 2-5 Adams merely discloses an upstream port and a downstream port. Again such teachings in Adams do not refer to any type of authentication or key exchange. Further, at column 5, line 61 to column 6, line 5 Adams merely discloses a header including source and destination, checksums, and option bits such as that which indicates that data are encrypted. That disclosure in Adams also does not even address any authentication or key exchange.

At column 6, lines 6-16 Adams merely discloses extraction of header information and comparison of an extracted header information with a key list at the time of encryption. That disclosure in Adams, however, also does not even address any authentication or key exchange. Also, at column 6, lines 21-29 Adams merely discloses a key list contains keys for encrypting/decrypting data and handling information. That portion of Adams, however, fails to even address any authentication or key exchange. Also, at column 6, line 65 to column 7, line 11 Adams merely discloses reconstruction of IP data packet using encrypted data. That disclosure in Adams, however, also fails to even address any authentication or key exchange.

In such ways, Adams fails to disclose or suggest any features related to contents protection procedure including at least an authentication and/or key exchange, and in such ways Adams does not disclose or suggest the features relied upon in the Office Action directed to the "contents protection information reception unit" and the "contents protection information transfer unit" of claims 1 and 2, the "first contents protection unit" and the "second contents protection unit" of independent claims 5, 11, and 19, the "copy protection

processing unit" of claims 12, 13, 14, and 16, and the "first copy protection processing unit" and the "second copy protection processing unit" of claim 17.

Moreover, as Adams does not even disclose the features relied upon in the Office Action, the basis for the outstanding rejections combining Adams with the teachings in Sato and Hitachi are also not believed to fully meet the limitations of the noted claims, and thus each of the outstanding rejections is traversed by the present response.

Moreover, as noted above each of independent claims 1 and 2 is amended by the present response to clarify an operation "to selectively relay the contents protection information transparently without making any change in the contents protection information". That feature is believed to further distinguish those claims over the applied art.

The relay device of claims 1 and 2 "transparently" relays the contents protection information, without making any change, while relaying the control command signals "non-transparently". No combination of teachings of Adams, Sato, and Hitachi discloses any relay device that selectively relays the contents protection information "transparently"; a "transparent" relay being simply passing information through the relay device without making any change.

In such ways, independent claims 1 and 2, and claim 4 dependent on claim 2, further distinguish over the applied art.

With respect to independent claims 5, 11, 17, and 19, those claims are amended by the present response to further recite that the claimed relay device carries out contents protection procedure separately with respect to the device/service/sub-unit on the first network and the device/service/sub-unit on the second network.

Specifically, the relay device in claim 5 carries out contents protection procedure including at least the authentication and/or the key exchange, separately with respect to the device/service/sub-unit on the first network and the device/service/sub-unit on the second

network, and the relay device receives the encrypted contents from one network side and re-encrypts the contents at the time of transferring the contents to the other network side.

The combination of teachings of Adams, Sato, and Hitachi clearly fails to disclose or suggest any relay device that carries out contents protection procedures separately and re-encrypts the contents at the time of the contents transfer. Thereby, claims 5-10 further distinguish over the applied art.

Independent claim 11 carries out contents protection procedure including at least authentication and/or key exchange, separately with respect to the device/service/sub-unit on the first network and the device/service/sub-unit on the second network, by using identical key information, and the relay device receives the encrypted contents from one network side and re-encrypts the contents at the time of transferring the contents to the other network side. The combination of teachings in Adams, Sato, and Hitachi clearly fail to disclose or suggest any relay device that carries out contents protection procedures separately by using identical key information and re-encrypts the contents at the time of the contents transfer. Thus, independent claim 11 further distinguishes over the applied art.

The relay device of independent claim 17 carries out contents protection procedure including at least authentication and/or key exchange, separately with respect to the device/service/sub-unit on the first network and the device/service/sub-unit on the second network, and receives the encrypted contents from one network side, converts its coding format, and re-encrypts the contents at the time of transferring the contents to the other network side. The combination of teachings of Adams, Sato, and Hitachi clearly fails to disclose or suggest any relay device that carries out contents protection procedures separately, converts the coding format of the received contents and re-encrypts the contents at the time of the contents transfer. Thus, independent claim 17, and claim 18 dependent therefrom, further distinguish over the applied art.

The relay device of claim 19 carries out contents protection procedure including at least authentication and/or key exchange, separately with respect to the device/service/sub-unit on the first network and the device/service/sub-unit on the second network, by referring to states of the contents reception unit and the contents transmission unit, and the relay device receives the encrypted contents from one network side and re-encrypts the contents at the time of transferring the contents to the other network side. The combination of teachings of Adams, Sato, and Hitachi clearly fails to disclose or suggest any relay device that carries out contents protection procedures separately by referring to states of the contents reception unit and the contents transmission unit and re-encrypts the contents at the time of the contents transfer. Thus, independent claim 19 further distinguishes over the applied art.

With respect to independent claim 12, independent claim 12 recites "a reception unit for receiving a query regarding a service/sub-unit/plug that is transferring the encrypted contents either through the virtual channel or by attaching the identifier, from said another device on the network". Independent claim 12 further recites "a notification unit for notifying a service/sub-unit/plug that is transferring the encrypted contents, to said another device on the network in response to the query". Independent claim 13 recites similarly "a transmission unit for transmitting a query regarding a service/sub-unit/plug that is transferring the encrypted contents either through the virtual channel or by attaching the identifier, to said another device on the network" and a "reception unit for receiving a notification regarding a service/sub-unit/plug that is transferring the encrypted contents, from said another device in response to the query".

With respect to claims 12 and 13 the Office Action recognizes that Adams fails to disclose such features regarding the authentication target query reply, and the outstanding Office Action cites the teachings in Perlman at column 14, lines 38-49 with respect to such

features. However, applicants respectfully submit such teachings in Perlman do not meet such limitations and thus do not overcome the recognized deficiencies in Adams.

Perlman at column 14, lines 38-49 merely describes a query from a network manager to each node to determine if the respective node has received a particular packet. Perlman fails to disclose or suggest any query and reply regarding a service/sub-unit/plug that is transferring the encrypted contents, to ascertain which service/sub-unit/plug is transferring the encrypted contents. In further maintaining the rejection to claims 12 and 13 the Office Action states:

> ...Perlman teaches basic querying for packet reception and responding with a confirmation (at least col. 14, lines 38-49). This reads on the claim of the reception unit receiving a query from another device on a network and notification unit for responding to the query. Combined with Adams' use of encryption of contents for transmission over the network, Perlman and Adams teach the basic principle of such an ACK and receipts type service for such querying.[2]

In response to the above-noted basis for maintaining the rejection, applicants submit the combination of teachings of Perlman and Adams at most implies an ACK and receipts type service for querying about whether a particular packet is received or not. Claims 12 and 13, in contrast to even such a combination of teachings, are not directed to such a basic principle of an ACK and receipts type service for querying in general, but are specifically directed to a querying as to which service/sub-unit/plug that is transferring the encrypted contents, and a combination of teachings of Perlman and Adams clearly fails to disclose or suggest such a specific querying about which service/sub-unit/plug is transferring encrypted contents.

Moreover, applicants respectfully submit Adams fails to disclose or suggest the "copy protection processing unit" of claims 12 and 13 as noted above.

---

[2] Office Action of February 11, 2005, page 31, last full paragraph.

In such ways, applicants respectfully submit claims 12 and 13 also distinguish over the applied art.

With respect to independent claim 14, independent claim 14 recites a communication device that transmits or receives encrypted contents through a flow, and carries out contents protection procedure including at least an authentication and/or a key exchange in units of the flow.

With respect to such features the outstanding rejection cites teachings in Adams at column 4, lines 40-52; column 5, line 65 to column 6, line 5; and column 6, lines 17-20 and 21-29.[3] However, applicants respectfully submit such teachings in Adams do not correspond to the claimed features.

At column 4, lines 40-52 Adams merely discloses a table to be used in making a routing or encryption/decryption decision, which includes keys for encrypting and decrypting data. That portion of Adams fails to disclose or even address any flow as well as any authentication or key exchange.

At column 5, line 65 to column 6, line 5 Adams merely discloses a header including source and destination, checksums, and option bits such as that which indicates that data is encrypted. That portion in Adams also clearly fails to even address any flow as well as any authentication or key exchange.

At column 6, lines 17-20 Adams merely discloses that a key list contains matching criteria such as source addresses and destination addresses. That portion of Adams also clearly fails to even address any flow as well as any authentication or key exchange.

At column 6, lines 21-29 Adams merely discloses that the key list contains keys for encrypting/decrypting data and handling information. However, that portion in Adams also fails to even address any flow as well as any authentication or key exchange.

[3] Office Action of February 21, 2005, pages 26-27, prenumbered paragraph 5.

In maintaining the rejection to claim 14 the outstanding Office Action states:

> It was well known in the art at the time the invention was made that a packet header contains a source/dest port/addresses as Adams teaches (at least col. 5, lines 65-67) and thus Adams clearly transfers data according to the header information. Such a flow, as the claims state, being identified by a set of a source address and port as well as a destination address and port, thus Adams clearly teaches such a "flow".[4]

In response to the above-noted basis for maintaining the rejection, applicants respectfully submit the teachings in Adams of transferring contents according to header information containing source/destination port/address is being erroneously interpreted as a "flow". Adams actually only mentions a source address and a destination address, and does not mention a flow, a source port, or a destination port. Applicants further note that a "flow" is a well known concept in the art for a set of data that share the identical source address, source port, destination address, and destination port, which will be transferred together. A mere transfer according to header information such as in Adams including a source address and a destination address is not a "flow" as would be clearly understood to one of ordinary skill in the art.

Moreover, claim 14 explicitly requires carrying out contents protection procedures in units of such a flow, and Adams fails to teach or suggest such any manner of carrying out contents protection procedures. In fact Adams completely fails to disclose any contents protection procedure.

In such ways, applicants respectfully submit independent claim 14, and claim 15 dependent therefrom, also clearly distinguish over the applied art.

With respect to independent claim 16, independent claim 16 is directed to at least one of an identifier of a service, a sub-unit, a virtual channel, or a plug and an identifier for

[4] Office Action of February 11, 2005, the paragraph bridging pages 31 and 32.

uniquely identifying encrypted content is attached to information exchanged in the contents protection procedure including at least an authentication and/or a key exchange.

With respect to such claimed features the outstanding rejection cites Adams at column 4, lines 40-52, and column 5, line 61 to column 6, line 5.[5] However, applicants respectfully submit such teachings in Adams do not correspond to the claimed features.

At column 4, lines 40-52 Adams merely discloses a table to be used in making a routing or encryption/decryption decision, which includes keys for encrypting and decrypting data. That portion of Adams clearly fails to disclose or suggest any identifier of a service, a sub-unit, a virtual channel, or a plug, or identifier for uniquely identifying encrypted contents, as well as Adams failing to disclose or suggest any authentication or key exchange.

At column 5, line 61 to column 6, line 5 Adams merely discloses that a header includes source and destination, checksums, and option bits such as that which indicates that data are encrypted. That portion of Adams clearly fails to even mention any identifier of a service, a sub-unit, a virtual channel, or a plug, or any identifier for uniquely identifying the encrypted contents, as well as any authentication or key exchange.

In maintaining the rejection to claim 16, the outstanding rejection states:

> ...Adams teaches various network layers inserting unique information into the packets to include an option bit for identifying and indicating to the receiving node, the status of the encryption of the contents prior to transfer of the contents (see col. 5 line 61 - col. 6 line 5). Thus Applicants arguments are not persuasive and the rejection stands.[6]

In response to that position for maintaining the rejection, applicants respectfully submit a status of the encryption could not identify a service, a sub-unit, a virtual channel, or a plug that carries out exchange of the encrypted contents as required in claim 16. Such a

[5] Office Action of February 11, 2005, page 28.
[6] Office Action of February 11, 2005, page 32, first full paragraph.

status of the encryption also cannot be used to uniquely identify encrypted contents by the transmitting side device as required in claim 16.

Moreover, claim 16 requires the identifier to be attached to information exchanged in the contents protection procedure, and Adams fails to disclose or suggest any use of such an identifier in a contents protection procedure. In fact Adams fails to disclose any contents protection procedure.

In such ways, claim 16 also distinguishes over the applied art.

Moreover, no teachings in Sato, Hitachi, and Perlman can overcome any of the above-noted deficiencies in Adams.

In view of these foregoing comments, applicants respectfully submit that each of the claims as currently written distinguishes over the applied art.

As no other issues are pending in this application, it is respectfully submitted that the present application is now in condition for allowance, and it is hereby respectfully requested that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870
Surinder Sachar
Registration No. 34,423

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

EHK:SNS\la

I:\ATTY\SNS\0039\00397378\00397378-AF.DOC